RADIO TV REPORTS, INC.

4701 WILLARD AVENUE, CHEVY CHASE, MARYLAND 20815 656-4068

FOR PUBLIC AFFAIRS STAFF

PROGRAM ABC Nightline STATION WJLA-TV ABC Network

DATE October 26, 1982 11:30 P.M. CITY Washington, D.C.

SUBJECT The Geoffrey Prime Case

TED KOPPEL: His name is Geoffrey Arthur Prime. He worked in Britain's super-secret General Communications Headquarters, better known as GCHQ. He is now facing trial for espionage that's believed to involve passing American intelligence to the Russians. And U.S. officials say it could be the worst security leak since World War II.

We'll focus on that story tonight as we talk with a former employee of GCHQ, with a British journalist who specializes in intelligence stories, and with the author of "The Puzzle Palace," a book about the U.S. National Security Agency.

* * *

KOPPEL: History does not record who it was or precisely when, but it is safe to assume that not too long after the telephone was put into commercial use, the first electronic eavesdropper gained access to information that he or she was never intended to have. From that modest beginning an empire was born, as the finest minds and a few of the most corrupt began what has been a never-ending battle between the electronic encoders and decoders, between those who protect secrets and those who unravel them.

Our story tonight deals with just such a battle. It is, as John McKenzie tells us, essentially a breakdown in British security, but one which has almost certainly had an equal, if not greater, impact on U.S. security.

JOHN MCKENZIE: It was early this summer when the British first heard of Geoffrey Prime. Prime was arrested and charged with sexually assaulting young girls. But soon police

charged him with something else -- spying. Specifically, he's accused of passing on useful information to the Russians during a 13-year period stretching from 1968 to 1981. If true, it could be the most damaging penetration of Western security since the Second World War.

Prime worked at the heart of Britain's intelligence-gathering operation, at this top secret base at Cheltenham, 100 miles west of London. With its electronic web of dishes and cables, Cheltenham eavesdrops on the rest of the world, on foreign radio and television and satellite transmissions, and, most importantly, on governments, especially the Russians. Almost all the information gathered here is then shared with the United States.

Prime was hired here as a Russian language expert. By the time he quit in 1977, he had reached the rank of advanced linguistic specialist, a rank that gave him access to plenty of sensitive information.

DUNCAN CAMPBELL: The Russians would know immediately which of their codes were broken. They would compare the communications. That gives them two options. One, they can seal up the loophole and defeat usually very costly, elaborate and lengthy exercises in crytoanalysis. Or they can play the much more likely game of disinformation, using, in fact, the whole complex technological apparatus of spying as a double agent, as a disinformation channel.

MCKENZIE: Disinformation fed through Cheltenham could have affected a whole assortment of American conclusions about the Soviet Union. Disinformation could, for example, alter perceptions of the Soviet military, of future troop deployments, or particular strengths and weaknesses. It could affect arms negotiations, influencing America's assessment of Soviet nuclear capabilities and intentions. It could have an impact on trade, as well, by distorting U.S. conclusions about what the Soviets have and what they need.

Just how much damage was actually caused in this particular case is uncertain. And that, as much as anything else, is what frustrates American intelligence officials. It's now months since the leak was first discovered, and the British apparently have still not supplied Washington with a complete account of what happened. In fact, British authorities are saying very little to anyone, publicly or privately.

In Parliament, Prime Minister Thatcher has been questioned about security breaches, but has decided to take her time before commenting. Even opposition parliamentarians are treading carefully.

MAN: All we have available to us, of course, are press statements. And it's the government's responsibility to give the country some substance in terms of a response to questions which we're putting so that we can get removed from merely speculation, or indeed inspired speculation, or indeed good investigative reporting, and get down to the hard facts of the government's responsibility, overall, for national security. It's up to the government to see that things are made watertight.

MCKENZIE: The case is now before the courts. So, by law, coverage here is limited. In fact, Prime's name has not been mentioned publicly since he was charged back in July.

Even American papers are not immune. The New York Times, which this Sunday reported on the impact of the case, suspended distribution in Britain so as not to be in contempt of court here.

ANNOUNCER: The news at 5:45 with Michael Nicholson.

MCKENZIE: For the time being, at least, the British are being told very little of the story.

MICHAEL NICHOLSON: The Attorney General, Sir Michael Havers, has declined to answer questions in the Commons about the alleged spy scandal at the Government Communications Headquarters at Cheltenham. He said the matter was sub judice. An American newspaper has claimed the Russians were able to get hold of highly sensitive information from Cheltenham in the 1960s and the 1970s. The Communications Headquarter is also used by the Americans.

MCKENZIE: Despite the low-keyed approach to this story here, there seems to be genuine concern within Britain's intelligence community, concern that Americans no longer trust them, and concern Americans have good reasons not to trust them.

KOPPEL: While the British Official Secrets Act makes just about any discussion of the Geoffrey Prime case illegal in England, there is no such restriction on broadcasts to this country. And in a moment we'll talk about the case live via satellite to London with a former employee of the General Communications Headquarters in Cheltenham, with a British journalist who specializes in intelligence matters, and, in this country, with the author of a new book on the U.S. equivalent of GCHQ, the National Security Agency.

* * *

KOPPEL: With us now live via satellite from our London Bureau is Alex Lawrie, an expert on African languages, who

worked for Britain's super-secret Government Communications Headquarters for 22 years. Also in London, Duncan Campbell, a writer for The New Statesman. He specializes in intelligence and was himself accused of violating Britain's Official Secrets Act for his research into GCHQ. And from our affiliate WCVB in Boston, James Bamford, author of "The Puzzle Palace," a book about this country's communications intelligence organization, the National Security Agency.

Mr. Lawrie, let me begin with you and let me ask you how it is -- perhaps it is we're misdescribing it when we talk about this super-secret government organization. How is it that, apparently, information was so easily taken out?

LAWRIE: Well, it's certainly very, very easy indeed for anyone to bring material out of GCHQ, because during the 22 years I was there I knew of no case in which anyone was searched, either going in or coming out. Nor were cars searched at all, to my knowledge. So it wouldn't have been beyond the wit of anyone who was so inclined to bring material out.

KOPPEL: Well, then that brings me back to the original aspect of my question. I mean are we making a mistake when we talk about it as being a super-secret organization?

LAWRIE: Oh, it's super-secret, all right. It's very difficult for outsiders to get to know very much about it. There's no doubt about that.

KOPPEL: Well, apparently it's not all that difficult. Or is there just this extraordinary, almost Alice-in-Wonderlandish kind of trust in all its employees?

LAWRIE: Well, I think there's an element of that in it. But I think some of those security procedures became fossilized with time. I think they may have been all right at one time, 20 or 30 years ago, but they haven't been adapted to changing circumstances.

KOPPEL: Now, I understand that you're not going to be able to discuss specifics with us, but what kind of material -- when you, for example, were translating material, what kind of material would that have been? Would it have been intercepts from public broadcasts or private telephone conversations, or any number of combinations?

LAWRIE: Well, I'm afraid I am subject to the Official Secrets Act until the day I die, so I can't be -- I can't be very helpful there.

KOPPEL: All right. So you cannot talk -- well, tell me

what you can't talk about, and then I'll see what's left.

LAWRIE: Well, I'll answer any reasonable questions on the state of security there and any apparent lapses there may have been.

KOPPEL: All right. Well, then let's talk about security in the sense that I find it incredible that for 22 years, if indeed this was the only lapse in security there -- during those 22 years that you were there, were there never any instance of someone stepping out of line and perhaps chatting with friends or relatives about material that he or she may have been handling there? Nothing that would have put people on guard, in other words, is what I'm trying to get at.

LAWRIE: Well, I think there would be evidence of that kind of thing. But I doubt whether it was taken seriously. The norm was for people to come in and go out from GCHQ without too much scrutiny. So I think the authorities there just grew to accept that as the norm.

KOPPEL: Mr. Campbell, you've spent a good part of your career writing about British intelligence. How is it possible that things could be treated with such complacency when in fact this material is so vital?

CAMPBELL: I think the problem with GCHQ and much of the British intelligence community is they have been long accustomed to the utmost protection from any kind of outside scrutiny, outside inspection, outside check to see that they stick by the spirit of their own, apparently, very stringent security rules.

KOPPEL: Well now, when you say they have been protected from it, let me then skip across the Atlantic to Mr. Bamford here.

Mr. Bamford, you have written extensively on the National Security Agency. The NSA, our super-secret organization deals very closely with GCHQ. Wouldn't you think that they'd be concerned about this lax security?

JAMES BAMFORD: Well, I'm sure they're very concerned about the lax security, because the NSA and the GCHQ are virtually partners in an organizational structure called the UKUSA agreement, the UK-USA agreement. And the two partners, GCHQ and NSA, exchange a great deal of information. In addition, they exchange personnel. There's NSA people today at GCHQ headquarters in Cheltenham and Cheltenham people at NSA headquarters at Ford Meade.

KOPPEL: All right. Let me ask you and Mr. Campbell both a question that will be difficult for you to answer with any precision, but give us the best you've got.

We have been referring to this and it has been referred to widely throughout the media as being one of the most serious breaches of security since the Second World War. If you agree with that, why?

CAMPBELL: I think it has to be said first that the exact details have yet to come out. And the British Government is doing all it can at the minute to cover up those details. But if you look at the career of Geoffrey Prime and the places he was in within GCHQ, he was in a position to handle a small but perhaps very significant proportion of the most critically sensitive material that the agency gets hold of. And that will...

KOPPEL: Why?

CAMPBELL: Well, because he was in the J Division, he was working as a Russian language specialist, and he was translating intercepts of Soviet communications, intercepts which might be picked up directly in open language, but would also include the hard-won code-breaking successes of both GCHQ and NSA analysts.

KOPPEL: What is the J Division?

CAMPBELL: It's the specialized signal intelligence division within GCHQ that deals almost exclusively with spying on the communications of Soviet bloc countries.

KOPPEL: Now, you explained, or at least we heard you explain in the recorded piece that we saw at the beginning of this program why it was that it would be so critical for the Russians to learn which of their communications had been cracked. Explain that in a little greater detail, would you, please?

CAMPBELL: The whole object of the game, if you are trying to be a superpower, is to keep your communications to your foreign embassies and military commands secret. The U.S. wants to do that. We want to do that. And the Russians want to do that. If an intelligence agency, like the NSA or GCHQ, is able to get into that communications system and read what's being said, understand what's being transmitted as it happens or shortly afterwards, you are in a diplomatically, militarily, or economically much more powerful position. And conversely, if the other side know that you are into that system, the opposite is true. You're being fooled.

KOPPEL: So, theoretically, it wouldn't even be necessary for Mr. Prime to be able to tell the Russians precisely what it was he had been translating, as long as he could give them a rough indication so they could go back and see, what, how it had been encoded?

CAMPBELL: I think if I were the Russian running Mr. Prime as a spy, as he's alleged to be, I would be quite happy just to see the bits of Russian that he was handling, because I could then go back through my own communications log of signals that one had sent, find out which signals had gone out on what channel, and deduce from that what places were intercepting it and whether secret codes were being broken.

KOPPEL: Mr. Bamford, back to you. And if you would look at it, please, from the American point of view. A serious security lapse?

BAMFORD: Yes, it's very serious. The NSA itself has had several major security lapses, back primarily in the early 1960s and mid-1960s. And this seems to top that. In the early 1960s, NSA had two analysts that defected to Moscow. That was probably the NSA's largest scandal. After that, there was an Army sergeant stationed at NSA headquarters who three years after he started was found out that he was selling secrets to the Russians, and for a good price. So there's no telling what he gave to the Russians. He was a messenger and had access to a great deal of information.

But in the Prime case, Prime was charged with 14 years of espionage, and he was a Russian linguist, a Russian translator. So I would think that his access was far greater than any of the NSA scandals.

KOPPEL: All right. But again, Mr. Bamford, if you would just explain to me -- these were fundamentally things that he was doing for the British. Why is that important to American intelligence or American national security?

BAMFORD: Well, the main reason is because the Soviet Union is obviously the United States' greatest target as far as eavesdropping goes. The United States shares information with the British in terms of code-breaking techniques, which circuits to monitor, and so forth. So that the British use a lot of NSA techniques in monitoring communications and breaking codes. As a result of that, Prime could have given to the Soviet Union a great deal of information about the NSA's own code-breaking techniques.

KOPPEL: Mr. Campbell, we have only a few seconds left. Explain to me quickly, if you can, how it is that Mr. Prime is

charged with 14 years of this business when, in fact, for the last three he was already out of GCHQ.

CAMPBELL: That's almost the billion-dollar question. No one has come up with a coherent explanation of why that seems to have been part of his alleged confession. But it's clear what the implications are. Either there was a spy ring then inside Cheltenham, and perhaps still operating; or the Russians set up a spy nest in Cheltenham or near to Cheltenham specifically to handle the gold mine that he may well have been producing.

KOPPEL: Mr. Campbell, thank you....

In a moment, a look at the secret world of electronic intelligence and what it's all about.

* * *

KOPPEL: The kind of spying we're focusing on tonight involves millions of dollars of the most elaborate and sophisticated electronic equipment and some of the most highly trained personnel involved in any kind of intelligence work. But it's purpose is relatively simple. Broadly stated, to overhear what the other fellow is saying.

James Walker reports.

JAMES WALKER: In Iran, a top secret American spy base that once eavesdropped on Soviet military communications. In the English countryside, a top secret Anglo-American listening post that monitors Soviet communications. And in the West Virginia hills, a top secret monitoring base that eavesdrops on satellite communications to and from the United States, as well as on Soviet satellites in deep space. All three were built as part of the worldwide intelligence campaign to intercept and decipher secret diplomatic, military and commercial information. It is a very aggressive, very surreptitious type of intelligence gathering, where the heroes fight not with bullets but with their brains.

The headquarters of America's electronic eavesdropping effort sits outside Washington, D.C. at the little-known National Security Agency. It is larger than the CIA, its budget in the billions of dollars. Its employees number over 100,000. The agency's building houses acres of computers that try to decode communications and record reports from secret satellites circling the earth.

How does it pay off? During the Falklands war American cryptanalysts reportedly broke an Argentine code detailing its military activities, then shared the crucial information with the

British.

But most success stories are seldom publicized. Take this machine, the top secret German Enigma cipher that Hitler used to send messages to his military command. Forty years ago the British cracked the code and warned that anyone who revealed their accomplishment would be shot. Their success remained a secret until ten years ago.

This is one of the original Enigmas used by the Germans during World War II. It was portable, easy to use, and the Germans thought it gave them a code what was impossible to break. Here's how it worked. Say you wanted to send a message that began with the word "attack." You type in the word and the machine scrambles the message, so attack becomes -- attack becomes jgugoy. But if you type it in again, the result is yeivnu. And every time you type it in, it'll come out differently.

The key was a combination of dials and plug settings inside the machine. Both the sending and receiving machine had to be exactly the same. What made the British task so difficult was that the settings were changed every day.

MAN: If we hadn't cracked the German Enigma signals, we just might not have won the war. And this is principally because the Enigma signals that were broken were immensely helpful in the battle of the North Atlantic, where the Nazi submarines were trying to sink Allied convoys going to Britain. By cracking these signals, the Allies knew how to avoid the wolf packs and, even more importantly, how to direct their aircraft and ships to sink these submarines.

WALKER: Though the technology has changed a lot since Enigma, the purpose remains the same. Electronic intelligence gives a nation an uncensored look into another nation's innermost thoughts, plans or actions.